

REMARKS

Applicants thank the Examiner for courtesy of an interview on February 9, 2006 and the following discussion regarding the prior art.

Applicants are submitting herewith new claims 13-28 that are believed to better distinguish the invention. In particular, the claims now more positively recite the invention as including steps of (a) defining a security perimeter, (b) defining one or more digital asset encryption policies which are applied to the digital assets when a risk of use of that digital asset occurs (i.e., by an end user) (c) if a sequence of digital asset access events matches a predefined digital asset usage policy that indicates a risk of use of the digital asset outside of the security perimeter, then (d) asserting a digital asset encryption policy by encrypting the digital asset prior to allowing access to the digital asset from outside the security perimeter.

It is believed that by emphasizing these features that indeed the prior art, U.S. Patent Publication 2003/01209350 (Teal), is better distinguished. In particular, Teal prevents intrusions into a kernel space such as by preventing overwriting of an operating system. Teal also has no notion of optionally applying an encryption policy based on attempted use of digital assets outside of a security perimeter. It also does not optionally encrypt files based on observed user level events. Indeed, Teal is always encrypting; it does not assert an encryption policy only if a certain observed sequence of events occurs.

According to Applicants' claimed invention, the assertion of encryption depends upon a proposed action to be taken with the digital asset. For example, one sequence of events described in connection with Figs. 7 and 8 of Applicants' specification detects a sequence of atomic level events (i.e., a local store) in which case no encryption action will be taken with the asset, and another sequence of events (i.e., forwarding an asset via web-based email) which will assert a policy in which encryption is applied. Even if Teal's operating system is considered to be a digital asset, Teal does not teach optionally applying encryption based on the result of detecting a sequence of events, based on that sequence.

And certainly, Teal is not detecting when the sequence of events indicates a risk of use of the digital asset outside of the security perimeter, as he is only encrypting the operating system components which are inside a security perimeter.

New claim 13 should thus be allowed.

We furthermore note that new claim 17 detects when the sequence of digital asset access events indicates that an end user is attempting to store a copy of the digital asset outside of the security perimeter, and the digital asset encryption policy specifies whether or not the digital asset is to be encrypted or not depending upon the type of storage device to which the copy is attempted to be stored. No such notion is contained in Teal or the other cited prior art references. Teal always encrypts. Teal does not optionally encrypt. Teal also does not optionally encrypt depending upon the type of storage device on which the copy is attempted to be stored.

Similarly, new claim 20 detects when an user is sending the digital asset outside of the security perimeter through a network communication port and the encryption policy specifies whether the asset is to be encrypted prior to the action of sending it.

Dependent claim 23 further brings out an optional aspect of Applicants' asserting of digital encryption policies. In particular, claim 23 requires that one of the policies specifies that encryption is to be applied to the asset when a particular sequence of access events is sensed, and another of the encryption policies specifies that encryption is not to be applied to the asset when another particular sequence of access events is sensed. Teal, as explained above, always applies encryption, regardless. It does not attempt to optionally apply encryption based on a sequence of access events. Thus, claim 23 is furthermore distinguishable over the prior art.

Claim 25 similarly asserts one of the digital encryption policies or not, depending upon the sensitivity of a particular asset.

The remaining claims are allowable for the same reason as the claims from which they depend.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By 

David J. Thibodeau, Jr.

Registration No. 31,671

Telephone: (978) 341-0036

Facsimile: (978) 341-0136

Concord, MA 01742-9133

Dated: 4/18/06